Claims

1. A method for a roaming user to establish a security association with an application server in a visited network, wherein the roaming user has completed a mutual authentication with a Bootstrapping Server Function (BSF) that performs user identity initial verification in a generic authentication architecture in his home network, and obtained a Bootstrapping-Transaction Identifier (B-TID) assigned to him by the BSF, comprising:

after receiving a service request message from the roaming user with the B-TID carried in the message, the application server in the visited network obtaining the roaming user's user information from the user authentication results of the generic authentication architecture in the roaming user's home network, establishing a security association with the roaming user.

2. The method according to Claim 1, wherein, the step of obtaining the roaming user's user information comprises:

the application server in the visited network sending a query message to an authentication entity in the local network to inquire the user information associated with the B-TID;

the authentication entity which received the message finding out the home network to which the user belongs according to the B-TID in the message, and acquiring the user information associated with the B-TID from the BSF in the roaming user's home network, and returning the acquired the user information to the application server;

the application server in the visited network obtaining the user information according to a response message returned from the authentication entity.

3. The method according to Claim 2, the authentication entity in the visited network is a BSF or a generic authentication architecture proxy in the visited network;

the step of the BSF or the generic authentication architecture proxy in the visited network acquiring the user information associated with the B-TID from the roaming

user's home network comprises:

the BSF or the generic authentication architecture proxy in the visited network directly sending a query message to the BSF in the roaming user's home network, inquiring the user information associated with the B-TID; and obtaining the user information associated with the B-TID from the response message returned by the BSF in the roaming user's home network.

4. The method according to Claim 3, wherein the generic authentication architecture proxy in the visited network is an independent server, or a server combined with an AAA server in the local network, or a server combined with the application server in the local network.

5. The method according to Claim 2, wherein, the authentication entiey in the visited network is the AAA server in the visited network;

the step of the AAA server in the visited network acquiring the user information associated with the B-TID from the BSF in the roaming user's home network comprises:

the AAA server in the visited network sending a query message to the AAA server in the roaming user's home network, inquiring the information assoiciated the the B-TID;

the AAA server in the home network inquiring the BSF in the local network, after the BSF in the local network finding the user information associated with the B-TID, it returning a response message, with the user information associated with the B-TID in it, to the local AAA server, and the AAA server returning a response message, with the user information associated with the B-TID in it, to the AAA server in the visited network; the AAA server in the visited network obtaining the user information associated with the B-TID from the response message returned by the AAA server in the roaming user's home network

6. The method according to Claim 1, wherein, the step of obtaining the roaming user's user information comprises:

the application server in the visited network notifing the roaming user that the B-TID is an illegal identity, and indicating the user to use a permanent identity;

having received the service request message from the roaming user again, with the permanent identity carried in the message, the application server in the visited network sending an authentication request to a AAA server in the local network; the AAA server in the visited network finding out the user's home network according to the user's permanent identity, and sending another authentication request to the AAA server in the roaming user's home network;

having received the authentication request from the AAA server in the visited network, the AAA server in the home network sending a request to the BSF in the local network for authentication of the user;

the BSF in the home network carring out mutual authentication with the user via the AAA server in the local network, the AAA server in the visited network and the application server in the visited network, after successful authentication, the BSF in the home network directly returning a successful authentication message carrying the user information to the AAA server in the local network, and the AAA server in the local network returning the successful authentication message to the AAA server in the visited network;

the application server in the visited network obtaining the roaming user's user information from the successful authentication message returned by the AAA server in the local network.

7. The method according to Claim 1, 2, or 6, wherein the user information comprises at least: key information and the user's identity.

8. The method according to Claim 7, wherein the user information also comprises the profile information associated with security.

9. The method according to Claim 7, wherein the key information is a shared key Ks generated in authentication, or a Ks-derived key and its valid term.